UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,518	04/01/2004	David Fultz	IDF 2564 (4000-15700)	8230

28003 7590 10/27/2009

SPRINT
6391 SPRINT PARKWAY
KSOPHT0101-Z2100
OVERLAND PARK, KS 66251-2100

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
10/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/815,518	FULTZ ET AL.	
	Examiner	Art Unit	
	SHANTO M. ABEDIN	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 June 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28 and 30-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28 and 31-33* is/are rejected.

7)☒ Claim(s) *30* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the communication filed on 06/16/2009.

2. Claims 1-28 and 30-33 have been presented for examination.

3. Claim 30 has been objected. Claims 1-28 and 31-33 have been rejected.

4. The examiner notes, upon further examination, new grounds for objections to claims are found, and presented in this office action.

Response to Arguments

5. The applicant's arguments regarding 35 USC 103(a) type rejections of claims 1-28 and 30-33 are fully considered, however, moot in view of the new grounds of rejection presented in this office action.

Claim Objections

6. Claims 1-8, 13-14, 28 and 30-33 are objected to because of the following informalities:

Regarding claims 1 and 28, they are directed to system comprising the components such as application program interfaces, authentication authority, and a store maintaining data etc. However, according to the specification (please see Par 038-046), these components could optionally be application or program modules, or be implemented in software or program only. Furthermore, claimed store maintaining data could optionally be a software implemented certificate authority or server! Therefore, claim languages raise an issue whether the claimed system actually includes any hardware components. Appropriate correction is suggested to avoid future 35 USC 101 type rejections.

Regarding claims 2-8, 28 and 30-33, they are objected because of their dependencies on the independent claims and failure to add any hardware component as part of the claimed system.

Regarding claims 13 and 14, they recite the limitations such as "information related to the token is token", or "information related to the token is a portion of data comprising the token" which seem to be indefinite in nature. In particular, claim languages seem to be recursive in nature, and it is not clear what exactly such information or portion of the data, or even the token is meant to be. The appropriate corrections are suggested to increase the clarity of the claim languages, and avoid any future 35 USC 112 second paragraph type rejection issues.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-8, 28 and 31-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Boydstun et al (US 7,334, 254)

Regarding claim 1, Boydstun et al discloses a system to provide application to application enterprise security for different applications on the different platforms where there

is no continuing context or session and a new context is created with new invocations from one of the application to another, the system comprising:

a security application program interface (Fig 2. 150: security API between security proxy and application server; Also communication interfaces between the security gatekeeper 220 and core security framework 250 could be interpreted as security application program interface) and an application program interface (Col 3, starts at line 45; Fig 2; interfaces in between the user and security gatekeeper or server; 140: application server, 230: SOAP server; interfaces coupled to the user, and the application or SOAP server is interpreted as application program interface) coupled to a client application on a first platform, the security application program interface operable to provide a security credential (Col 6, starts at line 22; user providing security information);

an authentication authority (Fig 2.250 or 120; core security framework, or policy server is interpreted as authentication authority) receiving the security credential from the security application program interface, the authentication authority further generates a token to the security application program interface where the security credential is valid, wherein the token contains user credential encoded as platform and application independent string data type (Col 4, lines 2-25, 48-60; Col 8, starts at line 30; token comprising security information; multi or cross-platform capabilities or security framework);

store maintaining data validating the security credential, the store in communication with the authentication authority to validate the security credential (Col 6, starts at line 40; Fig 2.10: security data store),

the platform program interface communicating regarding the validity of the token (Fig 2; Col 8, starts at line 25; communication between the security gatekeeper or proxy, and the core security framework regarding the validity of the token); and

a distinct server application on a second platform to receive the token from the application program interface, the server application communicating with the authentication authority to validate the token to enable the client application to use services of the server application (Col 6, lines 15-40; Col 8, starts at line 5; second enterprise, or the application server communicating with the core security framework regarding the validity of the token), wherein a new context is created with an invocation of the distinct server application by the client application (Col 6, lines 20-40; Col 8, starts at line 5; creating new security information, or token each time user request to access, or access the second enterprise/ server resources)

Regarding claim 2, Boydstun et al discloses the system wherein the server application further comprises:

an application program interface to communicate with the application program interface of the client application (Col 6, starts at line 40; Fig 2; communication interface between the security gatekeeper 220/ core security framework 250, or a second enterprise and user 210); and

a security application program interface to communicate with the authentication authority (Fig 2; Col 6, starts at line 25; communication interfaces between the security gatekeeper 220/ SOAP server 230/ second enterprise and the core security framework; core security framework is interpreted as authentication authority)

Regarding claim 3, Boydstun et al discloses the system wherein the server application caches the token after validating the token with the authentication authority such as that when the client application requests service of the server application, via the application program interfaces of the client application, the server application uses the cached token to validate the client application (Col 8, starts at line 25; using stored token for authentication)

Regarding claim 4, Boydstun et al discloses the system wherein the token generated by the authentication authority comprises a string including at least a portion of the security credential (Col 4, lines 2-25, 48-60; Col 8, starts at line 30; token comprising security information)

Regarding claim 5, Boydstun et al discloses the system wherein at least a portion of the token is in Extensive Markup Language format (Col 6, starts at line 40; XML, or SOAP compliant credentials)

Regarding claim 6, Boydstun et al discloses the system wherein at least a portion of the token is in Security Assertion Markup Language format (Col 6, starts at line 40; XML, or SOAP compliant credentials)

Regarding claim 7, Boydstun et al discloses the system wherein the token includes information related to an expiration date of the token (Col 6, starts at line 40; Col 7, starts at line 1; token and session/ time information)

Regarding claim 8, Boydstun et al discloses the system wherein validating the token by the authentication authority includes determining whether the authentication authority created the token (Col 4, lines 2-25, 48-60; Col 8, starts at line 30; authentication authority validating the token.)

Regarding claim 28, Boydstun et al discloses a system to provide application-to-application enterprise security for different applications on different platforms where there is no continuing context or session and a new context is created with new invocations from one of the application to another, the system comprising:

a first application program interface coupled to a first application on a first platform (Col 3, starts at line 45; Fig 2; interfaces in between the user and security gatekeeper or server; 140: application server, 230: SOAP server; interfaces coupled to the user, and the application or SOAP server is interpreted as application program interface)

a first security application program interface coupled to the first application on the first platform, to provide a first security credential (Fig 2. 150: security API between security proxy and application server; Also communication interfaces between the security gatekeeper 220 and core security framework 250 could be interpreted as security application program interface);

a second application program interface coupled to a second application on a second platform (Col 6, starts at line 40; Fig 2; communication interface between the security gatekeeper 220/ core security framework 250, or a second enterprise and user 210);

a second security application program interface coupled to the second application on the second platform, to provide a second security credential (Fig 2; Col 6, starts at line 25;

communication interfaces between the security gatekeeper 220/ SOAP server 230/ second enterprise and the core security framework; core security framework is interpreted as authentication authority);

an authentication authority receiving (Fig 2.120; Col 8, starts at line 26; core security framework) the first and second security credentials from the first and second security application program interfaces (Col 7, line 40 – Col 8, line 55; security information received from first and second enterprise/ gateway), the authentication authority further generating tokens and communicating the tokens to the first and second security application program interfaces where the first and second security credentials are valid, wherein the token contains user credential s encoded as a platform and application independent string data type (Col 4, lines 2-25, 48-60; Col 8, starts at line 30; token comprising security information; multi or cross-platform capabilities or security framework), wherein the tokens generated by the authentication authority are further defined as a first token generated by the authentication authority for the first application based on the first security credential and a second token generated by the authentication authority for the second application based on the second security credential (Col 6, lines 15-40; Col 8, starts at line 5; second enterprise, or the application server communicating with the core security framework regarding the validity of the token);

a store maintaining data validating the first and second security credentials, the store in communication with the authentication authority to validate the first and second security credentials (Fig 2.10; security data store).

the first application program interface communicating regarding tokens (Col 8, starts at line 25; user, or first enterprise application interface); and

the second application program interface receiving the token from the first application program interface (Col 8, starts at line 35; second enterprise application)

the second security application program interface (Fig 2; Col 6, starts at line 25; Col 7, starts at line 55; communication interfaces associated with the security gatekeeper 220/ SOAP server 230/ second enterprise gatekeeper) communicating with the authentication authority to validate the token to enable the first application to use services of the second application and wherein the second application receives the token from the second application program interface, the first security application program interface communicating with the authentication authority to validate the token to enable the second application to use services of the first application (Col 8, starts at line 25; second enterprise communicating with the core security framework regarding the validity of the first enterprise user token).

Regarding claims 31-33, they recite the limitations of claims 5-8 and 28, therefore, they are rejected applying as above applied rejecting claims 5-8 and 28.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 9-27 are rejected under 35 USC 103 (a) as being unpatentable over Upton (US 2003/0097574 A1) in view of Bhatia et al (US 7,249,375 B2) further in view of Silhavy et al (US 2005/0108521 A1)

Regarding claim 9, Upton discloses A method for providing application-to-application enterprise security for different applications on different platforms where there is no continuing context or session and a new context is created with new invocations from one of the applications to another, the method comprising:

coupling a security application program interface (Fig 4, Fig 5; Par 051, 061, 063, 069; container; application security services; security provider interfaces) and an application program interface to a client application on a first platform (Fig 4; Par 061-074, 127-130; container managed credentials; client application/ interfaces for storing, and providing security credentials);

communicating a security credential from the security application program interface to an authentication authority (Par 063, 074, 127-130, 150; client application/ interface providing credentials; 3rd party, or JAAS, or service provider interface/ SPI authenticating public/ password type, or generic/ token type credentials);

communicating information related to the security credential (Par 0061-0069; credentials; security-principle; ra.xml file containing security-principle) between the authentication authority and a data store to determine whether the security credential is valid; wherein the token contains user credentials encoded as a platform and application independent primitive data type (Par 104, 114, 130, 150; service provider interface/ SPI; validating/ authenticating credentials);

communicating the token (Par 0061-0069; credentials; security-principle; ra.xml file containing security-principle) to the client application; providing, by the application program interface coupled to the client application, the token to a server application, the server

application operable on a second operating system (Par 061-074, 127-130, 150; client application/ interface providing credentials; service provider interface/ SPI authenticating public/ password type, or generic/ token type credentials) ; and

validating, by the server application, the token before providing access to services of the server application by the client application (Par 0065-0069, 0104, 0114, 0130; storing credentials, or ra.xml file containing security-principle; SPI, or JAAS, or 3rd party validating/ authenticating credentials).

Generating a token, wherein the token contains user credential encoded as string data type (Par 063-065, 0150, 0065; storing, using token/ credentials, or ra.xml file)

Upton fails to disclose expressly generating a token by the authentication authority when the security credential is valid, wherein user credential encoded as a platform and application independent; and providing, by the application program interface coupled to the client application on the first platform, the token to a distinct server application, the distinct server application on a second platform.

However, , Bhatia et al teaches generating a token by the authentication authority when the security credential is valid (Fig 3; Col 3, starts at line 16; generating security token upon user authentication) , wherein the token contains user credentials encoded as a platform and application independent string data type (Fig 3; Col 3, starts at line 16; XML/ security token for authentication); providing, by the application program interface coupled to the client application on the first platform, the token to a distinct server application, the server application on a second platform; and validating, by the server application, the token before providing access to services of the server application by the client application (Fig 1, Fig 3; Col

3, starts at line 16; SSO enabled front end services uses token to access the backend-tier applications)

Alternatively, Silhavy et al discloses generating a token, wherein the token contains user credential encoded as platform and application independent string data type (Par 019, 028, 039 and 041; multi platform compatible token, credentials); and providing, by the application program interface coupled to the client application on the first platform, the token to a distinct server application, the distinct server application on a second platform (Fig 3; Fig 5; Par 019, 028, 039 and 041; Page 7, Col 2, lines 1-50). Silhavy et al further discloses a new context is created with new invocations from one of the applications to another (Fig 3.310, 330, Fig 4.460)

Silhavy et al, Bhatia et al and Upton are from the same field of endeavor of enterprise credential or access management. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Silhavy et al and Bhatia et al with Upton to design a method for enterprise security wherein the credentials are platform and application independent in order to provide a robust cross platform authentication mechanism.

Regarding claim 10, it is rejected applying as above applied rejecting claim 9, furthermore, Bhatia et al discloses the method wherein the distinct server application is provided with a security application program interface coupled to the distinct server application for validating the token with the authentication authority (Fig 1; Col 3, starts at line 45; RDBMS, or application services for validating the token with the SSO server.)

Regarding claim 11, Bhatia et al discloses the method wherein the application program interface coupled to the client application communicates the token to an application program interface of the distinct server application (Col 3, starts at line 3; user application).

Regarding claim 12, Bhatia et al discloses the method wherein validating the token by the distinct server application further comprises:

communicating information related to the token to the authentication authority (Fig 1; Col 3, starts at line 45; RDBMS, or application services for validating the token with the SSO server, or the credential/ token provider);

determining, by the authentication authority, whether the token is authentic (Fig 2; Col 3, starts at line 45; determining by the SSO server/ token provider whether token is authentic); and

receiving validation related information from the authentication authority (Fig 2; Col 3, starts at line 53; RDBMS receiving information about the token/ credential validity).

Regarding claim 16, Bhatia et al discloses the method wherein the authentication authority determines whether token is expired (Col 3, starts at line 25; verifying SSO session specific tokens)

Regarding claim 18, Bhatia et al discloses wherein the token includes a portion of the security credential in a string format (Col 3, starts at line 55; standard XML token)

Regarding claim 20, it is rejected applying as above applied rejecting claims 9 and 18. Furthermore, Upton fails to disclose using the encrypted token.

However, the examiner takes an official notice on that at the time of invention, using encrypted token for authentication purposes was well known in the art (See Bhat et al , US 2003/0200465 A1.) Therefore, it would have been obvious to a person of ordinary skill in the art to utilize the encrypted token for authentication purposes in order to provide better credential security.

Regarding claim 24, Upton discloses wherein the security credential is further defined as including a password and user identification (Par 061, 071, 074, 0150).

Regarding claim 25, it recites the limitations of claim20 and 24, therefore, it is rejected applying as above rejecting claims 20 and 24.

Regarding claim 26, Bhatia et al discloses the method wherein the security credential is an X.509 certificate and the data store is a certificate authority (Col 3, starts at line 55; use of certificates as credentials)

Regarding claims 13-15, 17, 19, 21-23, they recite the limitations of claims 9-12, 16, 18 and 20, therefore, they are rejected applying as above applied rejecting claims 9-12, 16, 18 and 20.

Regarding claim 27, it is rejected applying as above applied rejecting claims 9 and 26, furthermore, Bhatia et al discloses the method further comprising: communicating the X.509 certificate from the authentication authority to the certificate authority (Col 3, starts at line 55; SSO server or RDBMS optionally using token including PKI certificate); validating the X.509 certificate by the certificate authority (Fig 3; Col 3, starts at line 45; validating the token/ PKI certificate); and communicating validation information to the authentication authority (Col 3, starts at line 45; communicating the token/ certificate validation to the SSO server or back-tier application services).

Allowable Subject Matter

9. Claim 30 would be allowable if rewritten to overcome the objections to the claim, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to

37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 10:00 AM to 6:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195.

The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, AU 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436